ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, and instrumentalities of violations of 18 USC § 498, 18 USC § 1343, and 18 USC § 704(b)(d)(1), from the period November 1, 2018 through the present, including:

A. Records, communications, and tangible objects related to medical diagnoses and alleged military service.

B. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value to Sarah CAVANAUGH as an alleged military veteran.

C. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

i. evidence of who used, owned, or controlled the computer equipment;
ii. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
iii. evidence of the attachment of other computer hardware or storage media;
iv. evidence of counter-forensic programs and associated data that are designed to eliminate data;
v. evidence of when the computer equipment was used;
vi. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
vii. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage; and
viii. records evidencing the use of the Internet Protocol addresses to communicate over the Internet.

II. All computer hardware, computer software, and storage media, including cell phones or other devices that are or were previously assigned call number 401-

864-1535. Off-site searching of these items shall be limited to searching for the items described in paragraph 1.

BIOMETRIC ACCESS TO DEVICES

During the execution of the search of the Target Locations described in Attachment A, law enforcement personnel are also specifically authorized to compel Sara CAVANAUGH to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the Target Devices found at the Target Locations, and

(b) where the Target Devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Target Devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the Target Locations to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any Target Device. Further, this warrant does not authorize law enforcement personnel to request that Sara CAVANAUGH to state or otherwise provide the password or any other means that may be used to unlock or access the Target Devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Target Devices.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, mobile phone, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing

(such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols, and shall include any form of computer or electronic storage (such as flash memory or other media that can store data and any photographic form). including email, text messaging, instant messaging, or other communications, and including any content that may be synchronized to or on the device from any service or application utilized by the subject all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment

will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copies authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes